



Negeri Sabah, Malaysia

STATE GOVERNMENT ICT SECURITY POLICY

Copy right Sabah : 2004 by State ICT Security Working Committee,
Telephone : 088-256133
Fax : 088-215116
Web Site : www.SGcert.org
E-mail : team@sgcert.org
Version : 1.1
Date : 26th April 2005
All right reserved : No part of this documentation may be reproduced or processed, copied, distributed in any form without prior written consent of State ICT Security Working Committee, Sabah

TABLE OF CONTENTS

Foreword	i
State Government ICT Security Working Committee	ii
CHAPTER 1 INTRODUCTION	1
CHAPTER 2 OBJECTIVE	1
CHAPTER 3 POLICIES	2
3.1 Operation Security	2
3.1.1 Critical Systems	2
3.1.2 Systems Documentation	5
3.2 Data Transmission	8
3.2.1 E-Mail	8
3.3 Disaster Recovery And Business Resumption Plan	10
3.3.1 Disaster Recovery And Business Resumption Plan	10
3.4 Backup And Restoration	11
3.4.1 Workstation/Client Computer	11
3.4.2 Server	12
3.5 Physical Security	14
3.5.1 Perimeter Control	14
3.5.2 Access Control	16
3.6 Telecommunication	19
3.6.1 Backdoor Access To Sabah.Net	19
APPENDICES	
APPENDIX A TYPE OF THREATS	22
APPENDIX B ICT SYSTEM CHANGE FORM	23

FOREWORD

It has been recognized that information is a key for any development process and in this light, the Sabah State Government is committed to develop and enhance its Information Communication Technology (ICT) development to ensure an efficient and effective public sector services delivery to its clients while enhancing its global competitiveness. The Government wants everyone to have access to the wealth of ICT for it provides the powerful tools, which open up new opportunities for everyone.

The widespread use of ICT systems within the public sector has in turn led to a significant increase in the repository of intelligent assets of the government, which are now exposed to the vulnerability of open and networked electronic systems. Much has been done to ensure ICT security globally, but we cannot afford to be complacent. The Sabah Government ICT Security Handbook is intended as a reference and guide for public sector personnel in managing security in the implementation of ICT projects within Sabah's public sector as well as to compliment the Malaysian Public Sector Management of ICT Security Handbook (MyMIS), published on 15th January 2002 which the Sabah State Government has adopted.

I believe that this Sabah Government ICT Security Handbook lays knowledge and resource to yield a brief, usable and most importantly an understandable ICT security policy for all users in implementing an effective ICT security management in their respective locations. This Sabah Government ICT Security Handbook is a 'must read' source of information for everyone using ICT systems as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the organisation's critical system. Therefore, all relevant levels of management within the organization must be informed and understand the contents of this handbook which is meant to serve as the standard guide for all security management decisions and tasks to ensure business continuity, minimize business damage by preventing and minimizing the impact of security incidents and maximize business investments and opportunities in the targeted areas.

I thank and congratulate the Sabah State Government ICT Security Team and others involved in the publication of this timely handbook.

Datuk Peter Athanasius

*Deputy State Secretary (Development)
cum Chief Information Officer, Sabah*

State Government ICT Security Working Committee Members

1. **Datuk Peter Athanasius**
Ketua Pegawai Maklumat Negeri
Timbalan Setiausaha Kerajaan Negeri
2. **Dr. Mingu Hj. Jumaan**
Ketua Pegawai Keselamatan Negeri
Pengarah Jabatan Perkhidmatan Komputer Negeri
3. **Datuk Sukarti Wakiman**
Pengarah Jabatan Perkhidmatan Awam Negeri
4. **Datuk Felix Madan**
Timbalan Setiausaha Tetap (II)
Kementerian Kewangan
5. **Encik Bruno Vun**
Pengarah Unit Kemajuan IT Negeri
6. **Encik Yusuf Abdul Abbas**
Setiausaha Hal Ehwal Dalam Negeri dan Penyelidikan
Pejabat Hal Ehwal Dalam Negeri dan Penyelidikan
7. **Encik Mazlan Abdul Wahab**
Pegawai Keselamatan Kerajaan Malaysia Negeri Sabah
Pejabat Keselamatan Kerajaan Malaysia Negeri Sabah

Chapter 1 INTRODUCTION

In an effort to enhance the international competitiveness of the state and to improve the living standard of the people, the state public sector Information Technology Master Plan (ITMP) was formulated in 1997. The vision of the ITMP is to *achieve administrative renewal and bring the state closer to its citizen through a fully electronic government* and the mission is to *facilitate the reinventing of the government through strategic deployment of information and multimedia technologies*. The aim of the ITMP is to enhance the efficiency and effectiveness of the state public sector delivery of services as well as strengthening the decision making process. The ITMP as a guiding document, lays the foundation for the transformation of the operation of the state public sector through strategic deployment of information and communication technology.

Chapter 2 OBJECTIVE

In line with the state public sector vision and mission, a lot of application systems have been or are in the processes of being developed. Repositories have also been created for storing various types of information for easier and faster access from anywhere and at anytime. The systems are being used extensively in daily operation as the enabling tool to enhance the effectiveness and efficiency of the delivery of services.

With the advent of the Internet, threats such as malicious code, hacking and fraud (**see Appendix A**) are so common that not a single day passes by without reports of security incidents. In view of the criticality and confidentiality of the information created, the security of information within government systems is a major concern. In order to safeguard and prevent unauthorised access, damage and interference to information, ICT policies that provide adequate protection to state public sector ICT assets are needed to be put in place.

Chapter 3 POLICIES

3.1 Operation Security

What happens if the super-administrator of your critical systems got hit by a bus?

3.1.1 Critical Systems

Policy For any critical systems / applications there must be at least two persons who are well versed with the systems / applications and able to access, modify and operate them competently.

Standard Rotation of job must be enforced on operation of critical systems to make sure more than 1 person have the knowledge and ability to operate the systems.

Procedure Procedure to rotate job on operation of systems are as follows. Note: Steps (1) to (4) apply only to new personnel identified. Subsequently, only step (5) is necessary.

- (1) Identification and appointment of personnel
The management identifies and appoints person(s) to be the understudy of main person in charge of system. Identification should take into consideration the following factors: security and background vetting, level of basic expertise, interest, commitment, current workload and gender. This step should be completed within 1 week.
- (2) Adjustment / acclimatisation to role
The management briefs both the main person in charge of system and the newly appointed understudy on their role, responsibility

and time frame, placing specific emphasis on the objective of this exercise.

(3) Training

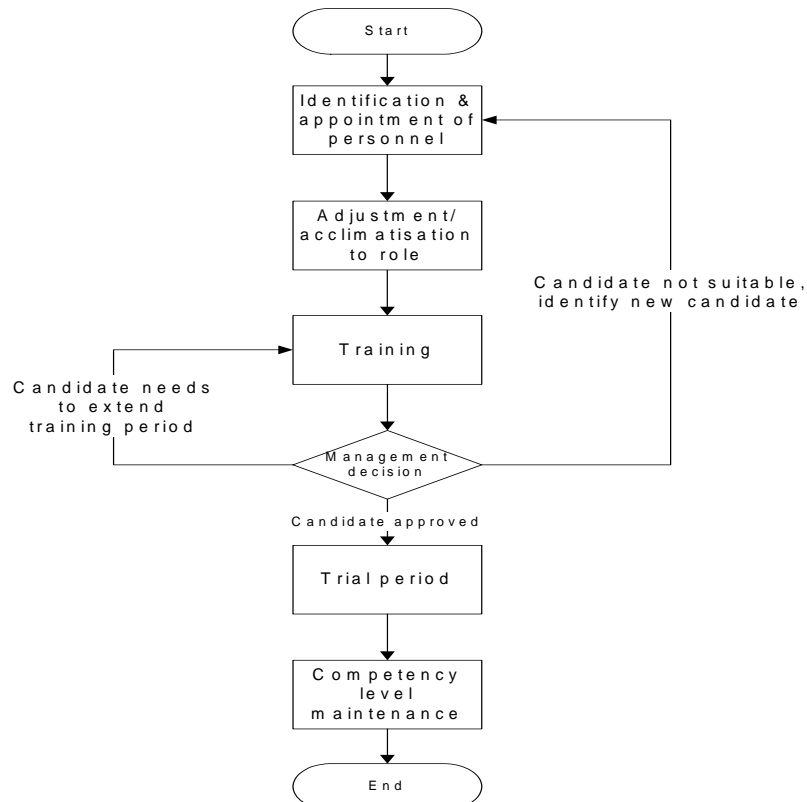
The appointed personnel undergoes intensive relevant training while accumulating on-the-job experience. The person in charge of the system will assess the competency level of the appointed personnel and report to the management on a weekly basis. Should the progress of the competency level of the appointed person not up to expectation within 3 months, the management would decide whether to extend the training period or repeat from step (1).

(4) Trial period

Upon reaching a satisfactory competency level, the appointed personnel handles the system for a period of time (as determined by the management) under the close supervision of the main person in charge of system.

(5) Competency level maintenance

At the end of the trial period, the administration of the critical system will now be rotated at least once a week among the persons in charge.



Guidelines

- (1) Repeat from step (1) of Procedure when there is a change in any of the persons in charge. Change in this case pertains to retirement, transfer, death, medically unfit, contravenes any provisions in Chapter D of Perintah Am Negeri Sabah or any condition which affects the performance of the individual.

- (2) The time frame for each step, if not specified, will be determined by the management as it deems fit.

3.1.2 Systems Documentation

Upgrading a server disabled access to SabahNet for everybody unexpectedly at 8.00 am on a Monday morning. What do you have to do to restore operations in the shortest time possible?

Policy Document any changes to any ICT system.

Standard All changes on any ICT system including the infrastructure must go through a change control management - recorded, tested, verified and approved - before being implemented. A back-out plan must also be in place to make sure a proper rollback if the need arises.

Procedure Procedure for change control management:

(1) Record any planned changes to ICT system

This should be done using a standard form (appendix A). The information should at least cover the following for the "current" and "after" states:

- Name/make/model of all ICT system involved.
- Version/build numbers of all ICT system involved.
- Name of personnel(s) who will carry out change.
- Purpose of change.
- Detailed steps to be taken to implement change.
- Date/time of plan of change.
- Date/time of testing of planned changes to a test system.
- Date/time of testing of back-out plan.
- Date/time of starting of change.
- Date/time of completion of change.

- (2) Verify and approve the request to proceed with test

The immediate superior officer of the personnel who is going to implement the change will decide on the request. If this request is not approved, no changes shall be made.

- (3) Test the planned changes to a test system/environment

This is to ensure operation is not affected in any way.

- (4) Prepare and test back-out plan

This is to make sure that changes can be reversed if the need arises.

The plan should at least cover the following:

- Hardware/software/personnel involved.
- Detailed steps to be taken.

- (5) Verify and approve the request to proceed with change

The immediate superior officer of the personnel who is going to implement the change will decide on the request. The officer can also request to repeat from step (3).

- (6) Announce time of change

This should be done well in advance to minimise downtime and effect on users. If need be, this change need to be done outside peak/office hours.

- (7) Implement the change

The start and end date/time of this step should be recorded.

- (8) IF THE NEED ARISES: carry out back-out plan

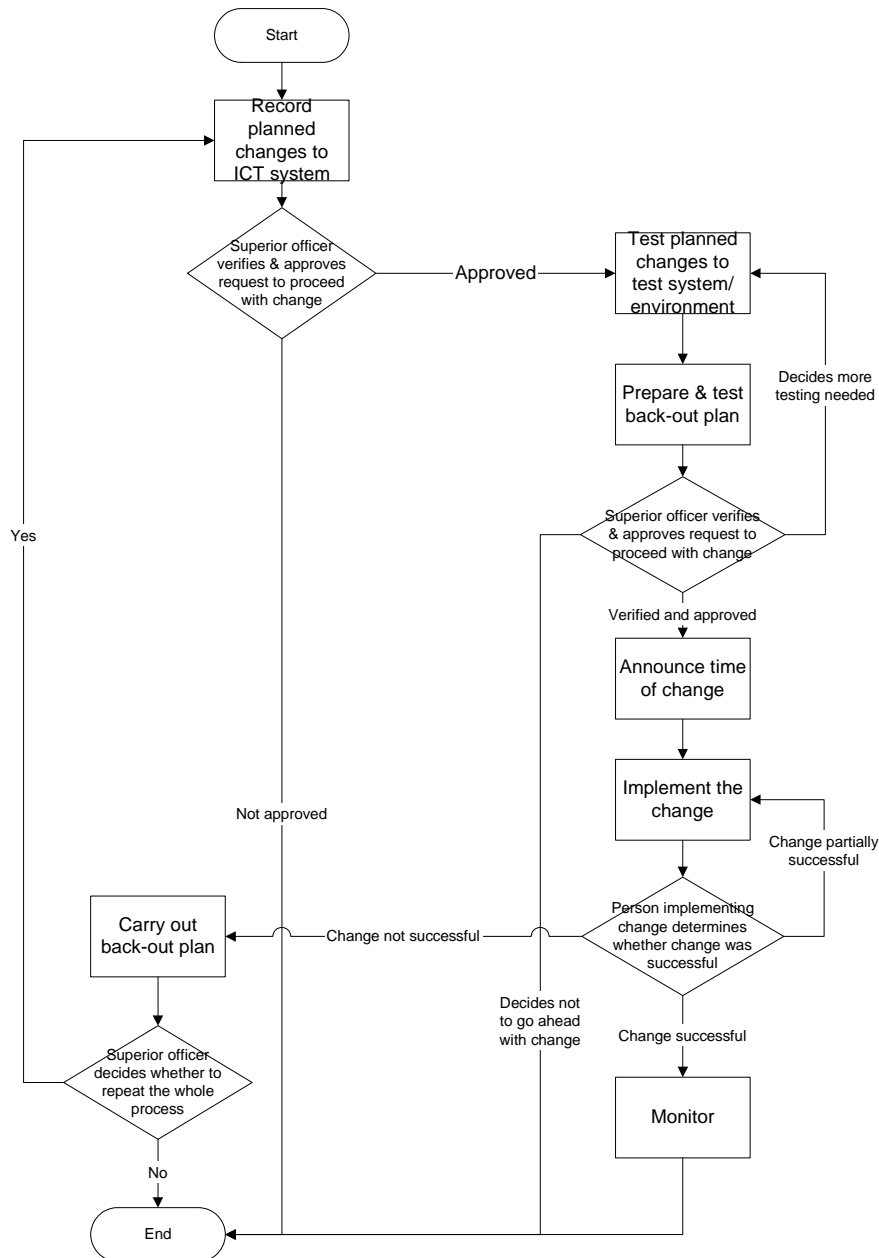
The following should be recorded as well:

- Why the implemented changes did not produce the desired results.
- System error messages.
- Steps to be taken to rectify the problem.

After carrying out the back-out plan, report back to the immediate superior officer to determine whether to repeat step (1).

- (9) Monitor

Monitor the implemented change for any effect it might have had on other related system(s).



Guidelines

- (1) During the planning stage, if the change is expected to take a long period, it should be broken down into smaller stages to minimise downtime.
- (2) If needed, all implementation of change should be done outside peak/office hours.

3.2 Data Transmission

What happens if an e-mail concerning a confidential matter has been tampered with along the way ?

3.2.1 E-mail

Policy All official e-mails must be transmitted in a secure manner to ensure **integrity**, **authentication** and **non-repudiation** on the part of the sender; and **non-denial of receipt** on the part of the recipient. In addition to that **confidentiality** for all classified official e-mails must be ensured also.

Standard All official e-mails must be signed using private key and all classified e-mails must be encrypted using public key before being sent. The minimum key length is 128 bits. For the purpose of compatibility , there should be only one asymmetric cryptographic system to be used throughout the state government. The sender must be notified of successful delivery of official e-mail.

Procedure Steps to use asymmetric cryptographic system for official e-mail transmission are as follows :

- (1) Register, Install and Publish Digital Certificate
 - Every government staff will be given a digital certificate, installed and published where necessary.
- (2) Sender Signs, Encrypts, and Sends E-mail

- Sender must ensure that all official e-mails are signed (and encrypted for classified e-mails), and set request for return receipt before sending.
- Sender must report to the mail administrator upon failure of receiving a return receipt within 5 working days.
- If any e-mail bounces back, the sender must refer to the mail administrator.

(3) Recipient Receives Signed and/or Encrypted E-mail

- Recipient must acknowledge the receipt of all official e-mails.
- Upon receipt of official e-mails which are not signed, the recipient must inform the sender to resend with a signed version.
- Upon receipt of e-mails which are suspected of being tampered with, the recipient must :
 - i report to sgCERT
 - ii inform the mail administrator
 - iii not do anything to the suspected e-mail
- Upon receipt of e-mails which are suspected of containing malware (e.g., viruses, worms, malicious code, etc.), the recipient must :
 - i inform the mail administrator
 - ii delete the e-mail

Guidelines

- (1) The cryptographic system used must be reviewed yearly or as and when deemed necessary by the government.
- (2) Classified e-mails are official e-mails which are categorized as "Rahsia Besar", "Rahsia", "Sulit" or "Terhad".
- (3) All e-mails bearing the sabah.gov.my domain are considered as official e-mails.
- (4) Refer to www.sgCERT.org for information on how to make reports to sgCERT.

3.3 Disaster Recovery & Business Resumption Plan

If your whole office burned down and all your ICT equipment are gone, how quickly can you restore your critical operations?

3.3.1 Disaster Recovery & Business Resumption Plan

Policy All organisations must have an appropriate disaster recovery plan in place for their ICT systems.

Standard The disaster recovery plan must enable the restoration and operation of the ICT systems within a time frame not exceeding 72 hours. All DRP must be reviewed, updated and tested at least once every six months.

Procedure

- (1) Organisation must adopt a standard backup methodology for their ICT systems. (refer to Data backup Policy)
- (2) Organisation must develop and test the DRP.
- (3) Upon completion of the DRP, a copy must be deposited with the sgCERT.

Guideline:

- (1) The guideline to setup a DRP for ICT can be obtained from sgCERT (www.sgCERT.org)

3.4 Backup And Restoration

On Friday night, the office catches fire and everything is destroyed. How much data will be lost?

3.4.1 Workstation

Policy All work related data in any computer must be stored in a central file server.

Standard All network computers shall have network directory mapped to the file server.

Procedure

- (1) System Administrator creates a directory for each user in the file server.
- (2) This directory has read/write permission for the user only
- (3) Map this directory as X: drive on user's computer

Guidelines

- (1) The definition of "work related data" and its level of importance to be stored in the file server is up to the discretion of the individual department. The work related data can include but not limited to:
 - a. Documents
 - b. Source code of In-house developed applications
 - c. Presentation / proposal
 - d. Letters
 - e. Email
- (2) All work-related data are to be stored on the mapped directory.

- (3) Any standalone computer, which holds important data, must have its own backup medium or means to copy the important data to the file server. (separate policy required)

3.4.2 Server

Policy All work-related data in all servers must be backed up.

Standard There must be two types of backup: Daily and Weekly. Daily backup (Differential or Full) must be done at suitable time giving minimum interruption to the operation of the department concerned. Full weekly backups must be done in two sets.

Procedure

- (1) Use appropriate backup & restore software and hardware / backup device.
- (2) Label all media properly with the following information:
 - a. Media ID
 - b. Volume no (x of y)
 - c. Description of Content
- (3) Perform backup with data verification.
- (4) Log the following information:
 - a. Department/Location
 - b. Media ID
 - c. Volume No (x of y)
 - d. Description of content (or Data Code)
 - e. Differential / Full
 - f. Daily / Weekly
 - g. Name of Backup Operator
 - h. Start Date/Time
 - i. Completion Date/Time
 - j. Server Name
 - k. Remarks

- (5) Keep the daily backup on-site.
- (6) Keep one copy of full weekly backup on-site for restoration and the other for off-site safe keeping.

Guidelines

- (1) Department concerned must verify that their backup is restorable.
- (2) It is up to the discretion of the individual department to determine the sufficient number of generations of backups for restoration of data integrity.
daily: keep 7 days.
weekly: keep 4 weeks.
monthly: =4th week. keep 12 sets.
yearly: =52nd week. keep 7 sets for 7 years.
- (3) The use of backup media, such as handling of tapes and the times of use, must be in accordance to the guidelines provided by the manufacturer.
- (4) Backup media include but not limited to the following:
 - a. Diskette
 - b. CDR / DVDR
 - c. Magnetic tapes (DAT / DLT)
 - d. Thumb drive
 - e. Hard Disk

3.5 Physical Security

What happens if a thief breaks into Government Office and steals classified data?

3.5.1 Perimeter Control

Policy Premises housing critical government information processing facilities must be protected from unauthorized access, damage and interference.

Standard Implement perimeter controls at all premises housing critical government information processing facilities.

Procedure

- (1) External walls constructed from the real ceiling where needed of premises housing critical government information processing facilities must be of solid construction.
- (2) Fire doors should be equipped with alarms and should automatically slam shut.
- (3) Buildings should be protected with secure doors, grills and locking hardwares where appropriate
- (4) Place a manned reception area or other means to control physical access to buildings. Access to buildings is restricted to authorized personnel only.

Guidelines

- (1) The criticality of the information processing facilities shall be decided by the organization concerned.
- (2) Solid construction for premises must follow construction/security standards based on :
 - i. JKR General Specification for Building Works.
 - ii. Arahan Keselamatan Negeri Sabah, Bab Keselamatan Fizikal (II-Keselamatan Bangunan)
 - iii. Relevant authorities Building-bylaws.

What happens if an unauthorized personnel enters Government premises and steals classified information?

3.5.2 Access Control

Policy All premises housing critical government information processing facilities should be designated as restricted areas.

Standard Access privileges for persons to restricted areas should be given on a need to enter basis.

Procedure

- (1) Those who need access to restricted areas must wear a security pass, of which type is determined by the following classification :
 - a. Permanent - Persons who work permanently in restricted areas must be issued with and wear a permanent security pass at all times.
 - b. Temporary - Persons who do not work permanently in restricted areas but require entry to carry out official duties must be issued with and wear a temporary security pass during the duration of the work.
 - c. Visitor - Persons from outside who are on official visit to restricted areas must be issued with and wear a visitor security pass and escorted by authorized personnel during the duration of the visit.
- (2) For each temporary and visitor entry, an access control log should be used to record the following information :
 - i. Name and NRIC number of the person(s) entering
 - ii. Employer or affiliation
 - iii. Name of the escorting person(s)
 - iv. Restricted area to be entered
 - v. Purpose
 - vi. Signature
 - vii. Date and time of entry
 - viii. Date and time of departure.
- (3) The number of visitors to restricted areas must be limited accordingly to minimize security risk.

- (4) The security pass must be returned upon exit from restricted areas.
- (5) Lost of security pass must be reported immediately.
- (6) Access controls should be applied at all restricted areas by using security identification mechanism such as swipe cards, biometrics, etc.
- (7) Surveillance devices such as CCTV, motion detectors and alarms should be installed in all restricted areas. The CCTV should be monitored at all times.
- (8) Installation of signs boards indicating "**authorized personnel only**" or a similar message should be prominently posted at all entrances to restricted areas.

Guideline

- (1) The criticality of the information processing facilities shall be decided by the organization concerned.

3.6 Telecommunications

A website hosted in a tightly protected network is suddenly defaced. The log files do not show any record of intrusion. How did the cracker managed to break into the highly secured network?

3.6.1 Backdoor Access to Sabah.Net

Policy Any connections that may establish a backdoor access to Sabah.Net is strictly prohibited.

Standard No backdoor access is allowed and any existing backdoor must be removed.

Procedure

- (2) All modems should be disabled or removed from desktop computer(s) which are connected to Local Area Networks (LAN).
- (3) Any desktop computer(s) that is/are found to have accessed the internet through back door access i.e. not via SabahNet must be disconnected and verified by ICT personnel to be clean before reconnecting to network.
- (4) All computers must have the most recent security updates, operating system patches, and antivirus patterns. For notebook computers, they must be installed with firewall.
- (5) Any unnecessary program(s) and service(s) which are not required to perform official job should be removed from computers to minimise risk of being compromised by malware or hacker.

Guidelines

- (6) Backdoor is a hardware or software-based hidden entrance to a computer system that can be used to bypass the system's security policies.
- (2) Backdoor connections include all non Sabah.Net access (e.g dial up access, broadband, leased line, wireless, etc).
- (3) Clean is defined as free from malware. Malware include but not limited to all types of viruses, worms, trojan horses, spywares, adware etc.
- (4) Security updates refer to any updates and hotfixes for any software used.
- (5) Firewall for notebook computers may include built-in firewall and the approved software list at <http://www.sgCERT.org/software>

TYPE OF THREATS

1. Adware
A program that carries advertisements usually in the form of a banner or as a pop-up in the screen. It may send information about the user to the originator of the program.
2. Brute Force Login
A program that uses exhaustive trial and error method to find the user authentication credentials in order to gain access to authorised area.
3. Denial of Service (DOS)
Disruption of network service by flooding the targeted site with heavy traffic.
4. Distributed DOS(DDOS)
A multitude of compromised systems attack a single target at the same time thereby causing denial of service for users of the targeted system.
5. Keylogger
A program that records every key strokes to a log file which can then be sent secretly to a specified receiver.
6. LAND Attack
A process whereby a SYN packet is sent to a host machine with the same source and destination ip address and port as if the host machine sent the packet to itself which will crash the host machine.
7. Packet Sniffing
A program that see and log all local network packets which may contain confidential data such as logon name and password.
8. Phishing
Email scam which uses an image that links to a site that purports to be a legitimate site. The linked site will ask for the user's information, credit card details, ATM Pin number etcetra.
9. Port Scanning
A process whereby excessive number of attampms to connect to ports on a specific destination ip address from the same source in order to locate an open, unprotected port.
10. Spamming
Unsolicited emails, most typically advertising.
11. Spoofing
A process whereby an unauthorised user uses the identity of an authorised user without permission.

12. Spyware A program that runs and collects data in the background without the knowledge of the victim. The collected data is then relay to advertisers or other interested parties.
13. SYN Attack A process whereby service is made unavailable by flooding the targeted site with connection requests from an invalid/spoofed address.
14. Virus Computer instructions that propagate itself into computer programs or data when it is executed within unauthorised programs.

Appendix B

ICT SYSTEM CHANGE FORM

ITEM	STATUS BEFORE CHANGE	ACTUAL STATUS AFTER CHANGE
Name/make/model of all systems involved		
Version/build numbers of all systems involved		
Name of personnel(s) who will carry out change:		
Purpose of change:		
Detailed steps to be taken to implement change:		
Date/time of plan of change:		
<p>Approval of request to proceed with test:</p> <p>.....</p> <p>Name:</p> <p>Date:</p>		
<p>Date/time of testing of planned changes to a test system:</p> <p>Remarks:</p>		
<p>Date/time of testing of back-out plan:</p> <p>Remarks:</p>		

Approval of request to proceed with change:

.....

Name:

Date:

Date/time of starting of change:

Date/time of completion of change:

Change confirmed successful:

.....

(Implementer)

Name:

Date:

.....

(Supervisor)

Name:

Date: